ISSN: 2278 – 909X
International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 5, Issue 4, April 2016

An Improved LSB Based Steganography Technique for Grayscale and Color Images

K.Dhinesh[1], K.Meenachi[2], A.Selvabharathi[3], S.Senthamilselvan[4]
[1]Assistant professor, Department of ECE
[2,3,4]UG Student, Department of ECE
Dr.Mahalingam College of Engineering & Technology
Coimbatore, India.

Abstract--This paper proposes an improved Least Significant Bit (LSB) based steganography technique in the spatial domain in that the secret information is hided in an image by altering small modifications in its pixels for imparting better information security. There is a wide variety of steganography techniques are available in that some of them are more complex than others and all of them have its respective pros and cons. we presently focusing on the case of grayscale and colour images are used as the cover images. Embedding the secrete message in the LSB bits of the images at random positions. This LSB method will have better embedding capacity and imperceptibility than the conventional methods. This LSB steganography ensures that the eavesdroppers will not have any suspicion that message bits are hidden in the image and hackers are not able to estimate hided message length. In addition to that it also ensures that the message can be retrieved completely even stego image get affected by stegano attacks.

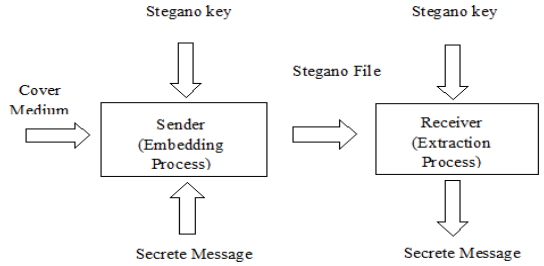
Keywords-- LSB, Steganography, Encoding, Imperceptibility, Embedding Capacity, Stegano Attacks.

I. INTRODUCTION

After the evaluation of communication system it is easy to share information among the world is very simple and easy. The sharing of information are takes place through both wired and wirelessmanners. Since the rise of internet one of the most important factors are considered in communication channel is secrecy of information. For secure communication cryptography was created as a technique and followed by different methods to encrypt and decrypt data in order to keep the message secret. Unfortunately sometimes the privacy of the information is not able to keep secrete by the conventional methods. In order maintain secrete of the information over the communication channel a new technique called steganography is emerged. Steganography is an art that can able to protect the information shared securely. Steganography is a technique that involves hiding a message in a suitable carrier e.g., an image, an audio or video file. In this technique the carrier carries the message secretly to the receiver[1]. Literally meaning "covered writing", it includes a broad collection of secret communication methods like undetectable inks, microdots, character organization, digital signatures, covert networks, spread spectrum etc. that conceal the very existence of message.An image steganography scheme is one kind of steganography systems, where the confidential message is hidden in a digital image with some hiding algorithm. Someone can then use a suitable embedding procedure to recover the hidden message from the image. The unique image is called a cover image in steganography, and the message implanted image is called a stegano image. Cover image, message and protection key are the constituents of steganography. The Steganos means covered or secret, and graphy means writing or drawing. Images can be more than what we see with our Human Visual System (HVS), because they can convey more than merely 1000 words. The basic image steganography has begun to work by replacing image bits with message bits. After that it gets evolved continuously with new ideas and configurations. The basic structure of the image steganography is follows:

1. Choose the cover medium has capable to carry the information securely.
2. Hide the message inside the image with a personal key for high security.
3. Stegano image is transmitted through the communication channel

Fig. 1. Flow Diagram of Steganography



The steganography is the art of embed secrete in a cover medium through this the information is transmitted. Encryption and decryption functions are also employed along with the steganography that ensures additional security. This can protect the information from the hacker who can able to modify the data encoded in an image. The cryptography is used with the steganography for confidential matters.

II. EXSISTING METHODS

A. Edge Least Significant Bit for Grayscale

Edge Least Significant Bit method, use all the edge pixels in an image. First calculate the masked image by masking the two LSB bits in the cover image. Identify the edge pixels by using the Canny Edge detection method[2,3]. After obtaining the edge pixels hide the data in the LSB bits of the edge pixels only and send the stegano object to the receiver. At the receiver, the stegano object is again masked at the two LSB bits. Then the canny edge detector is used to identify the edge pixels. Edge pixels at the sender and receiver are the same since the same masked image to calculate the edge pixels. Thus identify the bits where data is hidden. Message is obtained by extracting two LSB bits of the image in itsedgeareas. Replacing the least significant bits of the image at its edge areas is very popularly used algorithm.However, it is find that in most existing approaches, the choice of embedding positions within a coverimage mainly depends on a pseudorandom number generator without considering the relationship between the image content itself and the size of the secret message. Thus the smooth/flat regions in the cover images will inevitably be contaminatedafter data hiding even at a low embedding rate, and this will lead to poor visual quality and low security based on our analysis and extensive experiments, especially for images with many smooth regions. Then it leads to expand the LSB matching revisited image steganography and propose an edge adaptive scheme which can select the embedding regions according to the size of secretmessage and the difference between two consecutive pixels in the cover image. When the embedding rate increases, more edge regions can be released adaptively for data hiding by adjusting just a few parameters. The last bit in a pixel is called as Least Significant bit as its value will affect the pixel value only by “1”. So, this property is used to hide the data in the image. Here we have considered last two bits as LSB bits as they will affect the pixel value only by “3”. This helps in storing extra data. The Least Significant Bit (LSB) steganography is one such techniquein which least significant bit of the image is replaced with data bit.

B. Edge Pixel Replaced Randomly for Grayscale

In order to hide the secrete message in the last bytes of edge pixels randomly there is a need to generated a Pseudo random sequence which is used to choose the edge pixels[4,5,6]. There is an algorithm available to generate Pseudo random sequence of numbers, the elements of which is completely free of each other. The sequence generation uses the properties of arbitrary numbers hence the numbers are not truly random. Pseudorandom Number Generator (PRNG) functions are available to generate the required set of number. To make use of a PRNG, it first demands a seed. Seeding is the technical term for giving it an initial value, from which it can shoot out a sequence. If a PRNG is given the similar beginning, then it will give the same set of numbers every time and the

elements of which are approximately independent of each other. The outputs of pseudorandom number generators are not truly random – they only approximate some of the properties of random numbers. To use a PRNG, it first need a seed. Seeding is the technical term for giving it an initial value, from which it can shoot out a sequence. If a PRNG is given the similar seed, then it will give the same set of numbers every time.

C. Pseudorandom Method for Color Image

The Pseudorandom technique can shoot out the binary values by referring these values the message is encoded in a cover medium. By using the binary values the image steganography is employed. In simple word the technique is nothing but embedding the message in the random pixels of the cover medium. The number sequence is generated based on the seed value[7,8]. Initially seed pixel has to be chosen then sequence is formed with the reference of seed values. It replaces theoriginal pixel values of the cover image by the message values hence the steganoimage isobtained with the new set of values when compared with the original image values. Even though the new values are replaced the quality of the image is not get tainted. In general the generated pseudorandom sequence is need to transmit along with the stegano image to decode the secrete message without any mistakes.

D. 1:3:4 LSB Method for Color Image

In general any color image has the contribution of the primary colors. The factor that differentiates colors one from others of hue, saturation and intensity. Hence the least significant bit based steganography is going to employee in the least significant bits of all three components in RGB image[9,10]. Normally steganography is employed only at least significant bits of RGB image this leads to large variation in the pixel values hence the image gets degraded the identification of message on steganography image is also easy. Each pixels of the color image is contributed by the R-G-B contents. Red component contributes the most significant byte of the pixel. The green and the blue components contribute to least significant byte of the pixels. The new pixel value is formed by combining the changed red, green and blue components of the cover image then the stegano image is obtained. The embedding of message in the cover image is processed by sequence manner hence the retrieving of message at the receiver side is easy and also effective. Sequence embedding means that each pixel is split into R-G-B planes hence three planes are formed with respect to R-G-B then the values in these planes are nothing but the contribution of a particular component to a particular pixel values respectively. Embedding procedure in these plane involves, first the message bits are embedded in red component of a pixel then the next green component of the same pixel has been used and then the blue component of the pixel is changed after the completion of embedding the message values of the same pixel in three planes then the next pixels values are replaced by embedding further message bits.

III. PROPOSED METHOD

Improved LSB Method for Grayscale and Color Image

One of the most habitual techniques used in steganography nowadays is called least significant bit (LSB) insertion. This method is just what it sounds like; the least significant bits of the carrier-image then the information inserted. The letter or sequence of message is hidden in the pixels of image. After embedding, the LSB bit is change from ±1 from original pixel value. The message bits are replaced in least significant bits of RGB components of the cover image hence quality of image not get affected. This also improves imperceptibility and embedding capacity. During transmission of the stegano image affected by stegano attacks the message can be retrieved completely without any errors. This is also very effective algorithm even the image is affected by noise like salt and pepper.

A. LSB Embedding Procedure

If the LSB of pixel value I(i,j) is equal to message bit m to be embedded, I(i,j) remain unchanged; if not set the LSB I(i,j) to m. The message embedding procedure can be described using an equation as follows

$$Is(i,j) = \begin{cases} I(i,j)-1 & LSB(I(i,j))=1 \text{ ,m=0} \\ I(i,j) & LSB(I(i,j))=m \\ I(i,j)+1 & LSB(I(i,j))\neq 0,m=1 \end{cases} \quad ...(1)$$

Select the odd index pixel of image, if LSB of pixel is equal to message bit, the pixels remain unchanged. If the pixels value is not equal to message bit, pixel value is odd decrement by 1 else increment by 1.

B. LSB Extraction Procedure

Reverse process of embedding a message in image. Select the odd index pixel of image, pixel value is odd message bit is 1 else message bit is 0. By converting message binary stream to decimal, original message is retrieved.

if pixel value is odd

message bit is 1

else if pixel value is even

message bit is 0

IV. RESULTS AND DISCUSSION

The experimental results of the proposed and existing methods are discussed in this section. We have used MATLAB(8.1.0.604) for analysis. For the analysis of experiments MSE and PSNR measurements are considered. Mean square Error is measured between the cover and the stegano image. It is the measure of cumulative squared error between the images. Less value of MSE indicates that there is very less variations between the images. PSNR is often used to measure the quality between the original and reconstructed image. It is always measured in decibel. The higher the PSNR, better the quality of the reconstructed image. Formula for calculating the parameters are as follows

$$MSE = \frac{1}{MN}\sum_{m=0}^{M-1}\sum_{n=0}^{N-1}(X(i,j)-\hat{X}(i,j))^2 \quad ...(2)$$

dB

$$PSNR = 10\log\frac{255^2}{MSE} \quad ...(3)$$

Lena image of size 256x256 is taken as the cover image to embedded the secrete message. The existing and proposed improved LSB based steganography are employed in this standard lena image for experimental study.

Fig. 2. Standard Images for Experiment

The edge LSB method after embedding the message at the least significant bit of edge areas of the cover medium, the stegano image obtained is shown in the Fig.3.a. The payload capacity of this method depends on edge areas of the cover image, this increases when edge areas are more. MSE value is very low because very less variations between the images hence it has good imperceptibility. PSNR is good enough, the security is high. Even this has good security and not visible, the payload capacity is very less. Random edge last byte method embeds the message at the last bytes of pixels on random edge areas of the carrier, the obtained stegano image is shown in Fig.3.b. The payload capacity of this method is proportional to the edge pixels. The message is embedded at the last bytes there is a large variation on the pixel values between the cover and stegano image. Because of this MSE measure increases and PSNR is low. Increased value of MSE shows that this method is visible and lowered PSNR indicates that very less secured. The proposed improved LSB method encodes only at least significant bits of all the pixels of the cover image. Fig.3.c. shows the result of improved LSB. Because of changing values of pixels at its LSB only the deviation will be ±1. Since embedding at all the pixels of cover medium the payload capacity is very

high. MSE between the images is very low hence it is not visible. Higher value of PSNR indicates that it is much secured.

Fig. 3.a. Stegano image of Edge LSB

Fig. 3.b. Stegano image of Random edge

Fig. 3.c. Stegano image of Improved LSB

Table. 1. Parameter measures for Grayscale

Method	MSE	PSNR(dB)	Security
Random Edge	2.3691	44.3849	Less
Edge LSB	0.0070	70.0683	Better
Improved LSB	0.0061	70.2506	Good

The pseudorandom method embeds the message at random pixels of the cover image. The stegano image of this method is shown in Fig.4.a. Even the message is encoded randomly the pixel values varied only on Least significant bit. This results in less MSE values and PSNR is decent. The payload capacity of the method depends on the size of the image. Size of the image is high the payload capacity is also high. In the 1:3:4 method for color image, the stegano image is obtained after embedding in the above ratios on RGB planes. The resultant image is shown in Fig.4.b. The payload capacity of this method is depends on size of the message. When the size of the message is high the variation in pixels of RGB planes is also increased. MSE values gets increased but it is in the range of not predictable by human eye and PSNR is good enough to ensure the security. Improved LSB method embeds on LSB of all pixels of the color image and it is shown in Fig.4.c. The payload capacity is very high because in all the pixels are used for embedding the message. In this method large amount of data can able to encode. The variation between the stegano image and cover image is very low hence it lowers MSE value the imperceptibility is increased. PSNR value is very high then the security is improved. This method has high payload capacity and security. In addition to that the method is not visible.

Fig. 4.a. Stegano image of Pseudorandom

Fig. 4.b. Stegano image of 1:3:4

Fig. 4.c. Stegano image of Improved LSB

ISSN: 2278 – 909X
International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 5, Issue 4, April 2016

Method	MSE	PSNR(dB)	Security
Pseudorandom	0.0385	62.2741	Less
1:3:4	0.0502	61.1219	Better
Improved LSB	0.0043	71.7787	High

V. CONCLUSION

The proposed improved LSB method based steganography is an effective way to hide sensitive information secretly. This method has better imperceptibility and payload capacity than the available conventional steganography techniques. The robustness of message embedded in the cover medium is improved this shows that the method is very effective. The image persistence doesn't change much and is negligible when embedding the message into the image and the message is protected with the personal key. The results indicate that the improved LSB method has better PSNR of 10dB than the conventional ones. Size of the cover image and the stegano image will not vary even after the secrete message is embedded. The message secretly encoded is workable to retrieve in this improved LSB method. When the stegano image is affected by noise in communication channel and steganographical attacks also not possible to destroy the secrete message embedded in the cover medium hence this algorithm is very effective and has given better results when compared with festering methods.

VI. REFERENCES

[1] MamtaJuneja and Parvinder S. Sandhu, "An Improved LSB Based Steganography TechniqueFor RGB color Images," InternationalJournal of Computer and CommunicationEngineering, vol.2, no.4, 2013.

[2] Mrs. Kavitha, KavitaKadam, AshwiniKoshti,And PriyaDunghav, "Steganography Using LeastSiginificantAlgorithm," International Journalof Engineering Research and Applications(IJERA), vol.2,no.3,2012.

[3] Mr.VikasTyagi, Mr.Atulkumar, Roshanpatel,SachinTyagiand Saurabh Singh Gangwar ,"Image Steganography Least SiginificantBit With Cryptography," Journal of GlobalResearch in Science,vol.3,no.3,2012.

[4] A.D.Ker, "Steganalysisof LSB Matching inGrayscale Images," IEEE Signal ProcessingLetters,vol.12,no.6,2005.

[5] U.RizwanandH.Faheem Ahmed ,"A New Approach in Steganography Using Different Algorithmsand Applying Randomization Concept," International Journal ofAdvanced Research in Computerand Communication Engineering,vol.1,no.9,2012.

[6] NitinJain,SachinMeshram,Shikadubey, "Image Steganography Using LSB and Edge DetectionTechnique," International Journal of SoftComputing and Engineering(IJSCE), vol.2, no.3,2012.

[7] J.K.MandalandDebashisDas, "Colour ImageSteganography Based on Pixel Value Differencing in SpatialDomain," International Journal of Information Sciences andTechniques,vol.2,no.4,2012.

[8] Amanpreet Kaur,RenuDhirand GeetaSikka, "A New Image Steganography Based on First Component Alteration Technique,"InternationalJournal of Computer science and InformationSecurity,vol.3,no.6,2009.

[9] AtallahM.Al-Shatnawi, "A New inImage Steganography with Improved ImageQuality,"Journal of Applied MathematicalSciences,vol.6,no.79,2012.

[10] Mohammed Abbas Fadhil Al Husainy,"Message Segmentation to Enhance theSecurity of LSB Image Steganography,"International Journal of Advanced ComputerScience and Applications, vol.3, no.3, 2012.